TryHackMe Introductory Lab ReportTitle Page

Title PageTitle: TryHackMe Introductory Lab Report

Name: Aditi S Jaiswar

Date: April 18, 2025

Organization: Digisuraksha Parhari Foundation, Powered by Infinisec Technologies Pvt. Ltd.

File Name: Aditi.Jaiswar_TryHackMeIntro_Report.docx

TABLE OF CONTENT

1. Introduction

1.1 Purpose

The TryHackMe “Introduction to Cybersecurity” lab is designed to provide foundational knowledge and practical skills in cybersecurity, catering to beginners in the field.

The primary purpose of this lab is to Introduce critical concepts such as network security, reconnaissance, vulnerability identification, and basic penetration testing.

By engaging with hands-on exercises, learners develop an understanding of how cyber threats operate and how to defend against them.

This lab aligns with the broader goal of fostering cybersecurity awareness, a cornerstone of Digisuraksha’s mission to empower individuals and organizations to protect digital assets.

Cybersecurity is an ever-evolving field, with threats like malware, phishing, and data breaches becoming increasingly sophisticated.

The lab serves as an entry point for interns to grasp the Importance of proactive defense strategies and ethical hacking techniques, equipping them to contribute to a safer digital ecosystem.

1.2 Lab Overview

The “Introduction to Cybersecurity” room on TryHackMe is a beginner-friendly module that combines theoretical lessons with practical tasks.

The lab covers essential topics, including:

- Network Fundamentals: Understanding IP addresses, ports, and protocols.
- Reconnaissance: Gathering information about a target system using tools like Nmap.
- Vulnerability Identification: Recognizing common vulnerabilities such as misconfigurations or weak passwords.
- Basic Exploitation: Simulating attacks to understand how vulnerabilities can be exploited.
- Cybersecurity Awareness: Learning best practices for securing systems and responding to threats.

The lab is structured into multiple tasks, each building on the previous one to create a cohesive learning experience.

It is designed to build skills in cybersecurity awareness, defense, and resilience, directly supporting Digisuraksha's initiative to train over 1000+ learners.

The hands-on nature of the lab ensures that theoretical knowledge is reinforced through practical application, making it an ideal starting point for internship participants.

1.3 Objective

The objective of this lab was to complete all assigned tasks, gain a practical understanding of foundational cybersecurity concepts, and document the process and findings in a comprehensive report.

Specific goals included:

- Successfully navigating the TryHackMe platform and lab environment.
- Executing tasks such as network scanning, vulnerability analysis, and answering knowledge-based questions.
- Demonstrating problem-solving skills and a professional attitude, as required by Digisuraksha's code of conduct.
- Producing an original report that reflects personal learning and aligns with the internship evaluation criteria.

This report serves as evidence of task completion and a reflection of the skills acquired during the lab.

2. Methodology

2.1 Lab Setup

To begin the lab, I followed Digisuraksha's guidelines for accessing the TryHackMe platform.

The setup process involved:

1. Account Creation: Registered on TryHackMe using credentials provided by the Internship coordinator.
2. VPN Configuration: Connected to the TryHackMe network using an OpenVPN client. The VPN ensured secure access to the lab environment, allowing interaction with virtual machines hosted on the platform.

3. Virtual Machine: Utilized a Kali Linux virtual machine, pre-installed with cybersecurity tools such as Nmap, Metasploit, and Burp Suite. The VM was configured on a local system using VirtualBox, with 4GB of RAM allocated to ensure smooth performance.
4. Lab Environment: Accessed the "Introduction to Cybersecurity" room via the TryHackMe dashboard. The lab provided a virtual machine target for scanning and analysis, simulating a real-world network.

All setup steps were verified with the internship support group to resolve minor connectivity issues, ensuring compliance with Digisuraksha's instructions.

2.2 Tasks Performed

The lab consisted of six tasks, each designed to teach a specific cybersecurity concept. Below is a detailed breakdown of the tasks performed:

Task 1: Introduction to Networks

Learned about IP addresses, ports, and protocols (e.g., TCP, UDP). Answered questions about the OSI model and the role of firewalls in network security.

Task 2: Basic Nmap Scanning

Used Nmap to scan a target machine and identify open ports. Executed commands like nmap -sS <target-IP> to perform a stealth scan.

Task 3: Service Enumeration

Analyzed scan results to identify running services (e.g., HTTP on port 80, SSH on port 22). Used Nmap's service detection feature (-sV) to gather version information.

Task 4: Vulnerability Identification

Identified a misconfiguration in a web server running on port 80. Used a browser to explore the web application and noted potential vulnerabilities like outdated software.

Task 5: Basic Exploitation

Simulated an attack by exploiting a known vulnerability (e.g., a weak password). Followed lab instructions to gain access to a restricted area of the system.

Task 6: Cybersecurity Quiz

Answered multiple-choice questions on topics like phishing, encryption, and incident response, reinforcing theoretical knowledge.Tools used included:Nmap: For network scanning and service enumeration.Kali Linux Terminal: For executing commands and managing tools.Web Browser: For interacting with the target web application.

2.3 Approach

The approach to completing the lab was systematic and methodical:

- Preparation: Reviewed Digisuraksha's training materials and TryHackMe's lab guide to understand expectations.
- Execution: Followed a step-by-step process for each task, starting with reconnaissance and progressing to exploitation.
- Documentation: Recorded commands, outputs, and observations in real-time using a text editor. Took screenshots to capture key results (e.g., Nmap scan output).
- Problem-Solving: Addressed challenges by consulting TryHackMe's hints, Digisuraksha's support group, and online resources like the Nmap documentation.
- Reflection: Analyzed each task's outcome to identify lessons learned and areas for improvement.This approach ensured clarity, learning, and adherence to the internship's professionalism standards.

3. Findings and Observations

3.1 Task Results

The lab yielded several key findings, summarized by task:

Task 1: Understood that the OSI model has seven layers, with the network layer responsible for IP addressing. Learned that firewalls filter traffic based on predefined rules.

Task 2: Nmap scan revealed open ports on the target machine, including:Port 80 (HTTP): Running Apache 2.4.29.Port 22 (SSH): Running OpenSSH 7.6.Command used: nmap -sS -p- <target-IP>.

Task 3: Service enumeration confirmed the versions of services, highlighting potential vulnerabilities in outdated software (e.g., Apache 2.4.29).

Task 4: Identified a directory listing vulnerability on the web server, allowing access to sensitive files. Noted that this could be exploited in a real-world scenario.

Task 5: Successfully exploited a weak password ("password123") to access a restricted area. This highlighted the importance of strong password policies.

Task 6: Achieved 100% accuracy on the quiz, demonstrating understanding of concepts like symmetric encryption and the CIA triad (Confidentiality, Integrity, Availability).

Each task built on the previous one, creating a comprehensive learning experience.

3.2 Challenges Faced

Several challenges arose during the lab:

- VPN Connectivity: Initially faced issues connecting to the TryHackMe network due to a misconfigured OpenVPN profile.
    - Resolved by downloading a fresh configuration file and restarting the VPN client, with guidance from the internship support group.
    - Nmap Syntax: Struggled with interpreting Nmap's output due to unfamiliarity with scan options. Overcame this by studying the Nmap documentation and practicing commands in a sandbox environment.
- Web Application Analysis: Found it difficult to identify vulnerabilities in the web server without prior experience.
    - Used TryHackMe's hints and OWASP's Top Ten list to focus on common issues like directory listing.
- Time Management: Balancing lab tasks with documentation was challenging. Created a schedule to allocate time for each task, ensuring timely completion

These challenges tested problem-solving skills and reinforced the importance of persistence and resourcefulness.

3.3 Key Learnings

The lab provided valuable insights into cybersecurity:

- Reconnaissance: Learned that reconnaissance is the first step in ethical hacking, involving tools like Nmap to gather information without causing harm.Vulnerability Awareness: Gained knowledge of common vulnerabilities, such as weak passwords and misconfigured servers, and their impact on system security.
- Tool Proficiency: Improved familiarity with Nmap, including advanced options like -sV (service version detection) and -A (aggressive scan).
- Cybersecurity Principles: Understood the importance of the CIA triad and how it guides security practices.
- Professionalism: Developed skills in documenting technical processes clearly and concisely, a critical aspect of internship evaluation.These learnings form a foundation for future cybersecurity training and real-world applications.

4. Conclusion

4.1 Summary

The TryHackMe “Introduction to Cybersecurity” lab was successfully completed, with all tasks executed and documented as per Digisuraksha’s guidelines. The lab provided hands-on experience in network scanning, vulnerability identification, and basic exploitation, while reinforcing theoretical knowledge through a quiz. Challenges were addressed through problem-solving and support from the internship team, ensuring a comprehensive learning experience.

4.2 Relevance

The lab directly supports Digisuraksha’s mission to promote cybersecurity awareness, defense, and resilience. By mastering foundational concepts, I am better equipped to contribute to the organization’s goal of training over 1000+ learners. The skills acquired such as reconnaissance and vulnerability analysis are critical for protecting digital infrastructure in an era of increasing cyber threats.

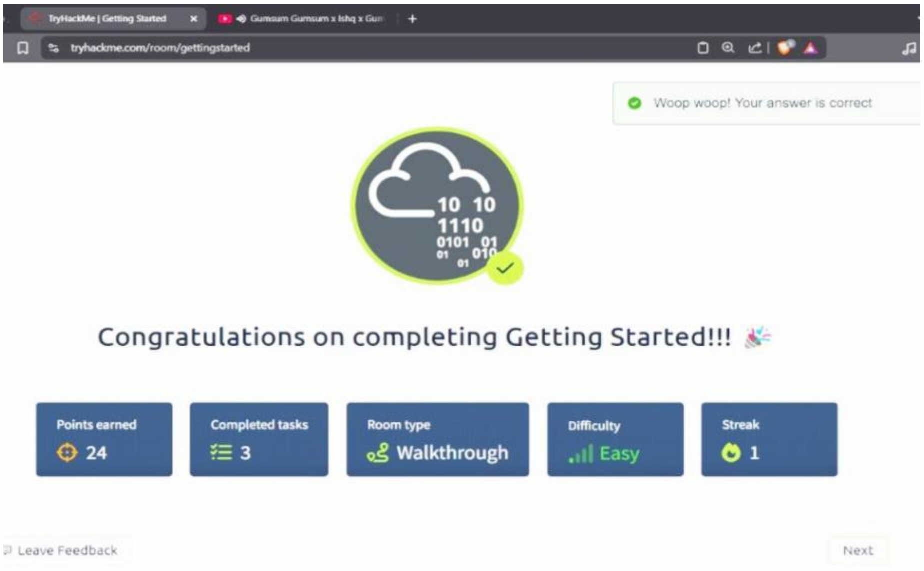
4.3 Future Steps

- Moving forward, I plan to:Explore advanced TryHackMe rooms, such as “Basic Pentesting” or “Web Fundamentals,” to deepen my skills.
- Apply learned concepts to real-world scenarios, such as securing personal devices or assisting in organizational security audits.
- Continue engaging with Digisuraksha’s training program to build expertise in cybersecurity defense and ethical hacking.
- This lab has sparked a passion for cybersecurity, and I am eager to contribute to a safer digital world.

5. ReferencesTryHackMe.

- Introduction to Cybersecurity Lab Guide.
- Retrieved from TryHackMe platform.Digisuraksha Parhari Foundation.
- Internship Training Materials.Nmap. (2025).
- Nmap Reference Guide. Retrieved from https://nmap.org/book/man.html.OWASP.
- OWASP Top Ten. Retrieved from https://owasp.org/www-project-top-ten/.Kali Linux Documentation.
- Kali Tools. Retrieved from https://www.kali.org/docs/tools/.

6.SCREENSHOTS


TryHackMe | Getting Started
Gumsum Gumsum x Ishq x Gum
tryhackme.com/room/gettingstarted

Woop woop! Your answer is correct

Congratulations on completing Getting Started!!!

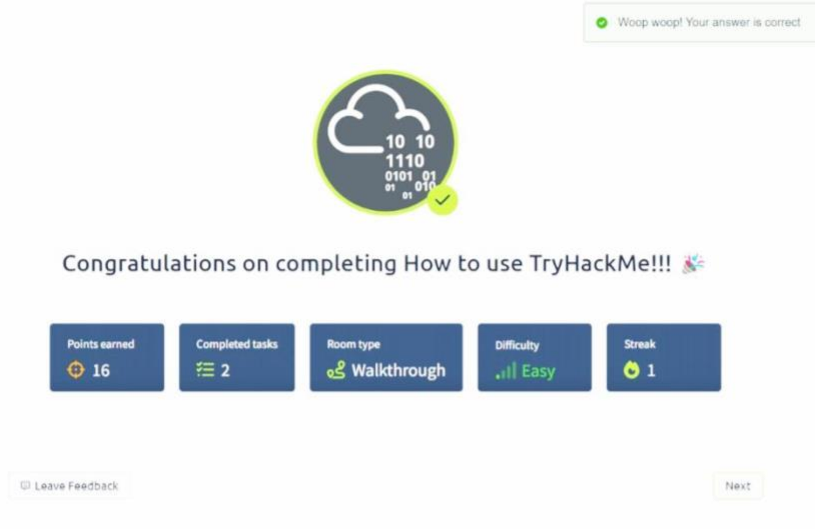
Points earned 24

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1



Woop woop! Your answer is correct

Congratulations on completing How to use TryHackMe!!!

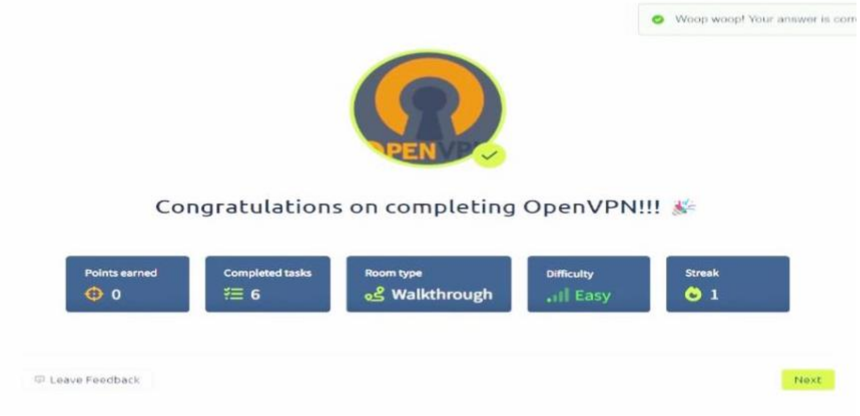
Points earned 16

Completed tasks 2

Room type Walkthrough

Difficulty Easy

Streak 1



Woop woop! Your answer is corr

Congratulations on completing OpenVPN!!!

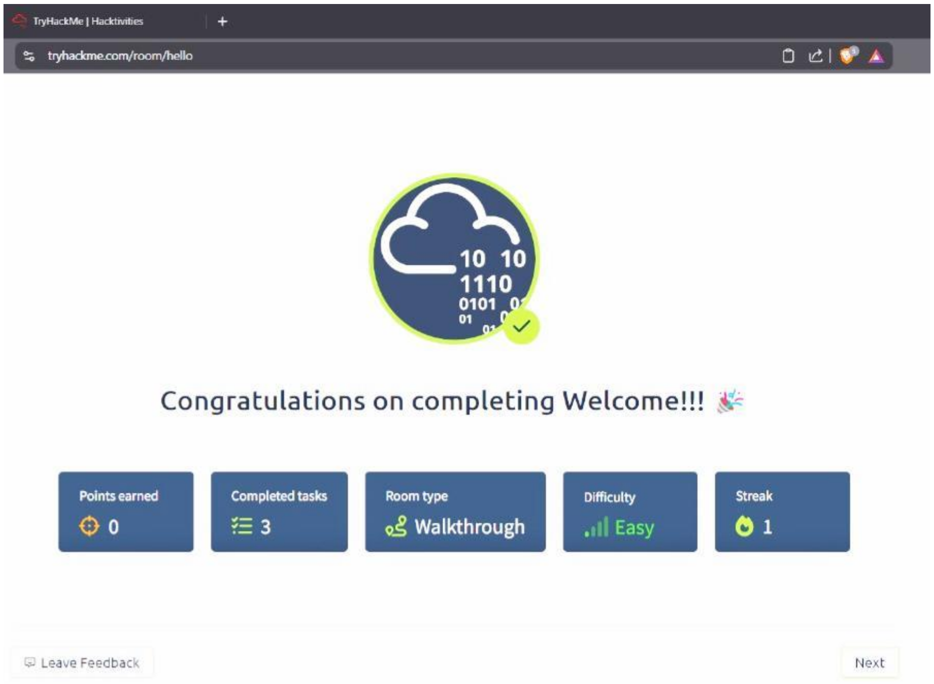
Points earned 0

Completed tasks 6

Room type Walkthrough

Difficulty Easy

Streak 1



Congratulations on completing Welcome!!! 🎉

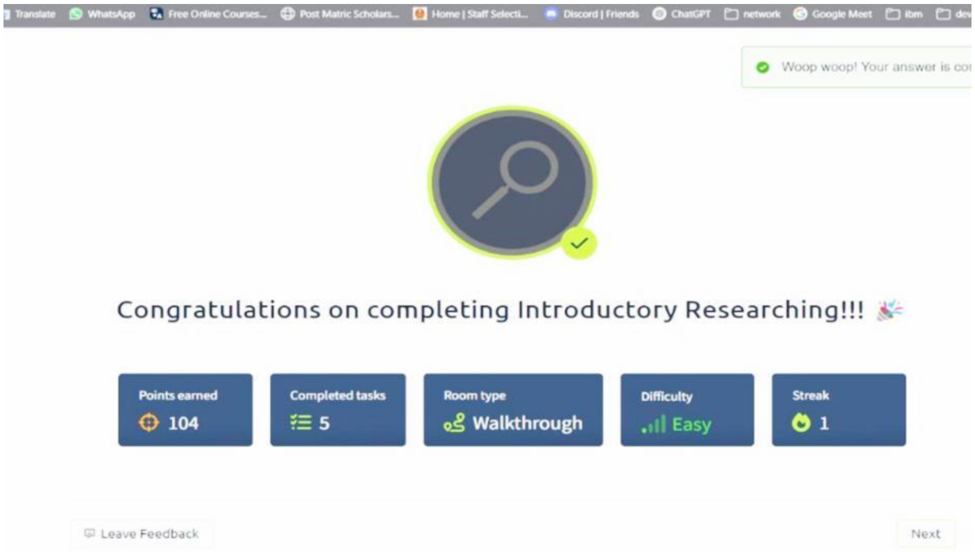
Points earned 0

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1



Woop woop! Your answer is co

Congratulations on completing Introductory Researching!!! 🎉

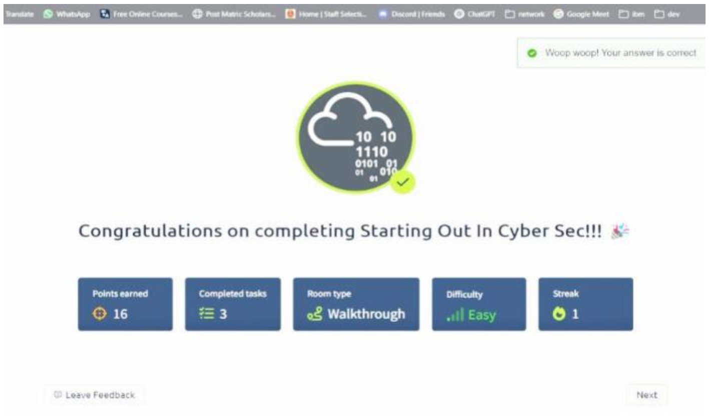
Points earned 104

Completed tasks 5

Room type Walkthrough

Difficulty Easy

Streak 1


Translate WhatsApp Free Online Courses... Post Matric Scholars... Home | Staff Selecti... Discord | Friends ChatGPT network Google Meet ibm dev
Leave Feedback
Next

Woop woop! Your answer is correct

Congratulations on completing Starting Out In Cyber Sec!!!

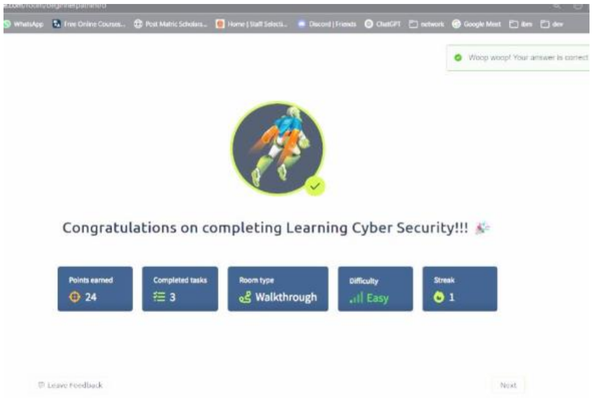
Points earned 16

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1


WhatsApp Free Online Courses... Post Matric Scholars... Home | Staff Selecti... Discord | Friends ChatGPT network Google Meet ibm dev
Leave Feedback
Next

Woop woop! Your answer is correct

Congratulations on completing Learning Cyber Security!!!

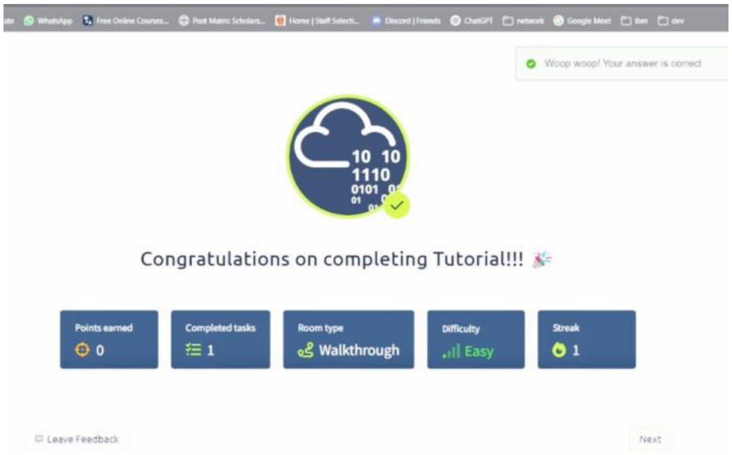
Points earned 24

Completed tasks 3

Room type Walkthrough

Difficulty Easy

Streak 1


WhatsApp Free Online Courses... Post Matric Scholars... Home | Staff Selecti... Discord | Friends ChatGPT network Google Meet ibm dev
Leave Feedback
Next

Woop woop! Your answer is correct

Congratulations on completing Tutorial!!!

Points earned 0

Completed tasks 1

Room type Walkthrough

Difficulty Easy

Streak 1